



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/849,318

05/19/2004

Paul Gassoway

063170.7177

5789

5073

7590

05/26/2010

BAKER BOTTS L.L.P.

2001 ROSS AVENUE

SUITE 600

DALLAS, TX 75201-2980

EXAMINER

LOUIE, OSCAR A

ART UNIT

PAPER NUMBER

2436

NOTIFICATION DATE

DELIVERY MODE

05/26/2010

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com

glenda.orrantia@bakerbotts.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/849,318	<b>Applicant(s)</b> GASSOWAY, PAUL	
	<b>Examiner</b> OSCAR A. LOUIE	<b>Art Unit</b> 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 06 April 2010.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                    | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)         | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                          |

Art Unit: 2436

## **DETAILED ACTION**

This final action is in response to the amendment filed on 04/06/2010. Claims 1-24 are pending and have been considered as follows.

### ***Examiner's Note***

In light of the applicant's remarks and amendments, the examiner hereby withdraws his previous 35 U.S.C 101 rejections. Additionally, upon further review of the applicant's disclosure, sufficient evidence was found to support the invoking of 35 U.S.C. 112 6<sup>th</sup> paragraph with respect to the "means for" claims, therefore the examiner has considered the applicant's "means for" claims in view of 35 U.S.C. 112 6<sup>th</sup> paragraph.

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-4, 7-10, 13-16, & 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1) in view of Coleman et al. (US-20050037733-A1).

Art Unit: 2436

Claims 1, 7, 13, & 19:

Vaidya discloses a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security comprising,

- “providing access to a database of signatures” (i.e. “the data repository 12 includes a database handler 26 which polls the data collectors 10 for intrusion detection data and stores the data for future reference”) [column 5 lines 47-50];
- “receiving data” (i.e. “The remote network 24 is connected to the LAN 11 and is equipped with a data collector 10 which monitors work stations located on the remote network 24 and transmits network security data specific to the remote network back to the data repository 12. Both the remote network 24 and the LAN 11 are connected to the global communications network referred to as the Internet”) [column 5 lines 39-46];
- “comparing the received data with the database of signatures” (i.e. “The attack signature profiles are adapted for detecting network data patterns associated with network intrusions which include unauthorized attempts to access network objects, unauthorized manipulation of network data, including data transport, alteration or deletion, and attempted delivery of malicious data packets capable of causing a malfunction in a network object”) [column 5 lines 33-39];

Art Unit: 2436

but, Vaidya does not explicitly disclose,

- “determining an initial system certainty value for the computer system,” although Coleman et al. do suggest a mistrust level for each wireless network device, as recited below;
- “each signature including a signature certainty value,” although Coleman et al. do suggest a confidence level with respect to a detected anomaly, as recited below;
- “increasing the system certainty value if the received data does not match a signature in the database,” although Coleman et al. do suggest , as recited below;
- “decreasing the system certainty value if the received data matches a signature in the database,” although Coleman et al. do suggest incrementing/decrementing the mistrust level accordingly, where although the incrementing and decrementing are done on inverse conditions as compared to the applicant's claims (i.e. the prior art decrements whereas the applicant increments under the same condition), Coleman et al. do suggest that the calculation methodology can be modified; additionally, it is reasonable to expect one of ordinary skill in the art to view the incrementing/decrementing as a design decision so long as the incrementing is opposite of the decrementing in terms of the matched conditions; that is, incrementing the mistrust level can be for a match so long as decrementing the mistrust level is for a no match and vice versa, as recited below;
- “filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data,” although Coleman et al. do suggest utilizing both the confidence value and initial mistrust level to calculate a new mistrust level to determine the intrusion prevention measures to enact, as recited below;

Art Unit: 2436

however, Coleman et al. do suggest , as recited below;

- "...The RIAFE 86 maintains a running mistrust level for each wireless network device 36, 38 and each WiAP 16, 16' in the WiNet 18 based on WiNet 18 traffic/event data 100 received at CDE 76. Based on the confidence metric and the type of anomaly detected (e.g., received as decision data from the CDE 76), different attacks are assigned different weights...For example, a detected RF anomaly is assigned weight .alpha. whereas a digital signature mismatch is assigned a different weight .beta.. The mistrust level of network devices 34, 36 and WiAPs 16, 16' is initialized to zero, then incremented and/or decremented by the RIAFE 86..." [page 6 para 102-103];
- "...The confidence level corresponding to the detected anomaly for that wireless network device..." [page 8 para 118];
- "...The RIAFE 86 maintains a running mistrust level for each wireless network device 36, 38 and each WiAP 16, 16' in the WiNet 18 based on WiNet 18 traffic/event data 100 received at CDE 76. Based on the confidence metric and the type of anomaly detected (e.g., received as decision data from the CDE 76), different attacks are assigned different weights...For example, a detected RF anomaly is assigned weight .alpha. whereas a digital signature mismatch is assigned a different weight .beta.. The mistrust level of network devices 34, 36 and WiAPs 16, 16' is initialized to zero, then incremented and/or decremented by the RIAFE 86...The mistrust level decrement value is calculated within the normal range of mistrust levels (e.g.,  $M < 4$ ) using CDE 76 inputs is illustrated with

Art Unit: 2436

the pseudo code in Table 4. However, the invention is not limited to this calculation and other calculations can also be used to practice the invention...” [page 6 para 102 & page 8 para 124];

- “...Also, the confidence metric is quantitative. In one embodiment of the invention, the confidence level is a real number between zero and one, and is used by the RIAFE 86 as a multiplier. However, the present invention is not limited to such a confidence level and other confidence levels can also be used. The confidence level corresponding to the detected anomaly for that wireless network device is multiplied by the weighting factor that is assigned to the corresponding detected anomaly, and the result is added to the existing mistrust level for the given wireless network device 36, 38 to arrive at the new mistrust level. A decrement value is also included. The mistrust level is adjusted according to Equation 9.  $M_{sub.new} = M + \alpha \cdot \beta \cdot M_{sub.dec.sub.--sub.val}$ , (9) where  $M_{sub.new}$  is a new mistrust level,  $M$  is an old mistrust level,  $\alpha$  is a confidence level in a detected anomaly,  $\beta$  is a weight assigned to the type of anomaly and,  $M_{sub.dec.sub.--sub.val}$  is a mistrust level decrement value...Pro-active intrusion prevention is achieved by dynamic switching or cycling of these protection suites according to the running mistrust levels. If a mistrust level of three is reached, more drastic intrusion prevention measures are taken, including switching of the RF band, for example, for 802.11b from 2.4 GHz to 5 GHz. This sends an alarm notification 102 to the network administrator 92...” [page 8 para 118-119 & page 9 para 130];

Art Unit: 2436

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining an initial system certainty value for the computer system" and "each signature including a signature certainty value" and "increasing the system certainty value if the received data does not match a signature in the database" and "decreasing the system certainty value if the received data matches a signature in the database" and "filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data," in the invention as disclosed by Vaidya for the purposes of adjusting the level of trust for a particular device based on the matches of anomalies/signatures (i.e. does the received data match a known intrusion).

Claims 2, 8, 14, & 20:

Vaidya and Coleman et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, their combination further disclosing,

- "the data that does not match a signature in the database is forwarded to its destination" (i.e. "indicating which network objects are not permitted to access other network objects") [column 6 lines 34-35].



Art Unit: 2436

Claims 3, 9, 15, & 21:

Vaidya and Coleman et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, but Vaidya does not explicitly disclose,

- “the increased or decreased certainty value becomes the initial system value,” although Coleman et al. do suggest incrementing/decrementing the mistrust level accordingly, as recited below;

however, Coleman et al. do disclose,

- “...The RIAFE 86 maintains a running mistrust level for each wireless network device 36, 38 and each WiAP 16, 16' in the WiNet 18 based on WiNet 18 traffic/event data 100 received at CDE 76. Based on the confidence metric and the type of anomaly detected (e.g., received as decision data from the CDE 76), different attacks are assigned different weights...For example, a detected RF anomaly is assigned weight .alpha. whereas a digital signature mismatch is assigned a different weight .beta.. The mistrust level of network devices 34, 36 and WiAPs 16, 16' is initialized to zero, then incremented and/or decremented by the RIAFE 86...The mistrust level decrement value is calculated within the normal range of mistrust levels (e.g.,  $M < 4$ ) using CDE 76 inputs is illustrated with the pseudo code in Table 4. However, the invention is not limited to this calculation and other calculations can also be used to practice the invention...” [page 6 para 102 & page 8 para 124];

Art Unit: 2436

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the increased or decreased certainty value becomes the initial system value," in the invention as disclosed by Vaidya for the purposes of adjusting the level of trust for a particular device based on the matches of anomalies/signatures (i.e. does the received data match a known intrusion).

Claims 4, 10, 16, & 22:

Vaidya and Coleman et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, their combination further disclosing,

- "the data comprises a packet of data" (i.e. "data packets") [column 5 line 38].

3. Claims 5, 11, 17, & 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1) in view of Coleman et al. (US-20050037733-A1) in view of Nakae et al. (US-20040172557-A1).

Claims 5, 11, 17, & 23:

Vaidya and Coleman et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, but their combination do not explicitly disclose,

Art Unit: 2436

- “the filtering further comprises forwarding the data if the signature certainty value is less than the system certainty value,” although Nakae et al. do suggest the confidence level exceeding the threshold value, as recited below;
- “the filtering further comprises discarding the data if the signature certainty value is greater than the system certainty value,” although Nakae et al. do suggest blocking access when the confidence does not exceed the threshold, as recited below;

however, Nakae et al. do disclose,

- “After the confidence level  $c$  has exceeded the threshold value  $T$ , the IP packets of the access from the ordinary host 302 are guided to the server 401 on the internal network 4” [page 11 para 193 lines 16-19];
- “This causes input IP packets to be continuously guided to the decoy unit. Thereafter, when detecting an attack corresponding to "intrusion" or "destruction", the permanent access blocking is made active” [page 14 para 249 lines 7-11];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “the filtering further comprises forwarding the data if the signature certainty value is less than the system certainty value” and “the filtering further comprises discarding the data if the signature certainty value is greater than the system certainty value,” in the invention as disclosed by Vaidya and Coleman et al. for the purposes of providing a determination as to whether a requester is permitted or denied access to the network according to a level of trust.

Art Unit: 2436

4. Claims 6, 12, 18, & 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1) in view of Coleman et al. (US-20050037733-A1) in view of Nakae et al. (US-20040172557-A1) in view of Moran (US-7032114-B1).

Claims 6, 12, 18, & 24:

Vaidya, Coleman et al., and Nakae et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, but their combination do not explicitly disclose,

- “the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded,” although Moran does suggest an event record, as recited below;

however, Moran does disclose,

- “an intrusion detection system comprises a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file, filter out expected time steps, correlate them with other events, and assign a suspicion value to a record associated with an event” [column 4 lines 28-33];

Art Unit: 2436

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded," in the invention as disclosed by Vaidya, Coleman et al., and Nakae et al. for the purposes of recording timed information for future further analysis.

### ***Response to Arguments***

5. Applicant's arguments filed 04/06/2010 have been fully considered but they are not persuasive.

- The applicant's remarks with respect to, "Applicant respectfully disagrees. These mistrust levels correspond to individual levels associated with & wireless network device located within a computer system. There is no disclosure, teaching, or suggestion of a single initial system certainty value for the computer system" have been carefully considered but are non-persuasive;
  - o The examiner notes that the "mistrust levels" associated with each "wireless network device" can be considered the "system certainty value for the computer system"; that is, the prior art teaches keeping track of multiple "system certainty values" one for each device (i.e. one for each system) and not just merely for one system;
- The applicant's remarks with respect to, "Coleman fails to disclose, teach, or suggest "increasing the system certainty value if the received data does not match a signature in the database" and "decreasing the system certainty value if the received data matches a

Art Unit: 2436

signature in the database." While Coleman does disclose incrementing and decrementing the mistrust levels, Applicant respectfully contends that these changes are not based on either matching or not matching signatures" and "Therefore, the decrementing process disclosed in Coleman is based only on timing, manual intervention, or re-authentication, There is no disclosure, teaching, or suggestion that matching or not matching a signature plays any role in this step" have been carefully considered but are non-persuasive;

- The examiner notes that given the broadest most reasonable interpretation, "matching signatures" specifically the "signatures" can be any criteria that are deemed as an intrusion that is then matched or determined to be a known intrusion.

### ***Conclusion***

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2436

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Friday from 8:30 AM to 5:00 PM. The examiner can also be contacted via E-mail to schedule a telephone discussion at OSCAR.LOUIE@USPTO.GOV.

If attempts to reach the examiner by telephone or E-mail are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is only available through Private PAIR. If you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100 (local). For more information on the PAIR system or the EBC please visit <http://www.uspto.gov/patents/ebc/index.jsp>. If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000 (local).

/OSCAR A LOUIE/  
05/21/2010

/Nasser Moazzami/  
Supervisory Patent Examiner, Art Unit 2436